UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/725,208	12/02/2003	Masato Yamamichi	2003_1741A	4485

52349 7590 04/16/2008

WENDEROTH, LIND & PONACK L.L.P.
2033 K. STREET, NW
SUITE 800
WASHINGTON, DC 20006

EXAMINER	
LOUIE, OSCAR A	

ART UNIT	PAPER NUMBER
2136	

MAIL DATE	DELIVERY MODE
04/16/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/725,208	YAMAMICHI ET AL.	
	Examiner	Art Unit	
	OSCAR A. LOUIE	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *04/19/2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-39,41 and 42* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-39,41 and 42* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This second non-final action is in response to the amendment filed 04/19/2007. In light of the applicant's amendments and arguments the examiner hereby withdraws his previous 35 U.S.C. 101 rejections regarding Claims 39 & 42 and statutory Double Patenting between applications 10725102 and 10725208. Upon further consideration, and in light of the applicant's arguments, the examiner has found it necessary to present this second non-final action with a new grounds of rejection. The examiner acknowledges the cancellation of Claims 40 & 43. Claims 1-39, 41, & 42 are pending and has/have been considered as follows.

Claim Objections

1. Claims 1-4, 6, 10, 20-22, 24, 28, & 37 are objected to because of the following informalities:

- Claims 1-4, 6, 10, 20-22, 24, 28, & 37 recite "operable to" which should be "…configured to…" Appropriate correction is required.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

3. Claims 3, 38, & 39 are rejected under 35 U.S.C. 102(b) as being anticipated by Gennaro et al. (US-5937066-A) herein known as Gennaro-066.

Gennaro-066 disclose a shared-key generation apparatus, a method used in a shared-key generation apparatus, and a program embodied on a computer readable storage medium and used in a shared-key generation apparatus that notifies a destination apparatus about a shared key in secrecy comprising,

- "a seed-value generating unit operable to generate a seed value" (i.e. "Alice and Bob exchange a random S (step 902)") [column 17 line 27];
- "a shared-key generating unit operable to generate a blind value and a shared key, from the seed value" (i.e. "Alice derives from S a value KG for each agent, by hashing S and the respective agent's ID (step 904)") [column 17 lines 29-30];
- "an encryption unit operable to encrypt the seed value based on the blind value, to generate encryption information" (i.e. "Alice encrypts the KG values under the respective agents' public keys (step 906)… PUa1: public key for Alice's first agent…KGa1: key-generating key for Alice's first agent") [column 17 lines 31, 32, 41, & 46];

- "a transmitting unit operable to transmit the encryption information" (i.e. "Alice sends to Bob the SKR phase 1 data block B1 (FIG. 11) composed of: T1, ePUa1(KGa1), ePUa2(KGa2), ePUb1(KGb1), and ePUb2(KGb2) (step 908)") [column 17 lines 33-35].

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1, 21, 41, & 42 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gennaro et al. (US-5937066-A) herein known as Gennaro-066 in view of Gennaro et al. (US-5907618-A) herein known as Gennaro-618.

Claim 1:

Gennaro-066 disclose a key agreement system comprising a shared-key generation apparatus and a shared-key recovery apparatus, each apparatus establishing therein a same shared key in secrecy comprising,

- "the shared-key generation apparatus includes: a seed-value generating unit operable to generate a seed value" (i.e. "Alice and Bob exchange a random S (step 902)") [column 17 line 27];
- "a first shared-key generating unit operable to generate a blind value and a shared key, from the seed value" (i.e. "Alice derives from S a value KG for each agent, by hashing S and the respective agent's ID (step 904)") [column 17 lines 29-30];

- "an encryption unit operable to encrypt the seed value based on the blind value, to generate encryption information" (i.e. "Alice encrypts the KG values under the respective agents' public keys (step 906)… PUa1: public key for Alice's first agent…KGa1: key-generating key for Alice's first agent") [column 17 lines 31,32, 41, & 46];
- "a transmitting unit operable to transmit the encryption information" (i.e. "Alice sends to Bob the SKR phase 1 data block B1 (FIG. 11) composed of: T1, ePUa1(KGa1), ePUa2(KGa2), ePUb1(KGb1), and ePUb2(KGb2) (step 908)") [column 17 lines 33-35];
- "the shared-key recovery apparatus includes: a receiving unit operable to receive the encryption information" (i.e. "Optional Transmission of S or K: If needed, SKR can transmit either or both S and K") [column 19 lines 3-4];
- "a second shared-key generating unit operable to generate a decryption blind value and a decryption shared key, using the decryption seed value and according to a same method as used in the first shared-key generating unit" (i.e. "Alice derives from S a value KG for each agent, by hashing S and the respective agent's ID (step 904)") [column 17 lines 29-30];
- "a re-encryption unit operable to encrypt the decryption seed value based on the decryption blind value, to generate re-encryption information" (i.e. "Alice encrypts the KG values under the respective agents' public keys (step 906)… PUa1: public key for Alice's first agent…KGa1: key-generating key for Alice's first agent") [column 17 lines 31,32, 41, & 46];

but, they do not disclose,

- "a decryption unit operable to decrypt the encryption information, to generate a decryption seed value," although Gennaro-618 do suggest a hash, as recited below;
- "a judging unit operable to judge, based on the encryption information and the reencryption information, whether the decryption shared key should be outputted," although Gennaro-618 do suggest verification based on at least one hash, as recited below;
- "an outputting unit operable, when the judging unit has judged affirmatively, to output the decryption shared key," although Gennaro-618 do suggest verification, as recited below;

however, Gennaro-618 do disclose,

- "from Alice (step 1002), Bob locates the previously cached values KGa1-KGb2, using the hash value Hash(B1) in the block B2 as an index (step 1004)" [column 14 lines 3-5];
- "if there are multiple sets of key recovery agents as in the present example, then Bob must ensure that all of the various versions of K agree if he is to fully validate the recovery information" [column 14 lines 25-28];
- "As disclosed in the copending Gennaro et al. application, the decryption procedure 1200 may be keyed to the receiver verification steps so that the message is not decrypted unless all or a specified subset of the key recovery fields in data block B1 and B2 have been verified" [column 14 lines 51-56];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "a decryption unit operable to decrypt the encryption information, to generate a decryption seed value" and "a judging unit operable to judge, based on the encryption information and the reencryption information, whether the decryption shared key should be outputted" and "an outputting unit operable, when the judging unit has judged affirmatively, to output the decryption shared key," in the invention as disclosed by Gennaro-066 since it is reasonable to expect that Gennaro et al. would combine elements from both of his own inventions for the purposes of decryption and verification.

Claims 21, 41, & 42:

Gennaro-066 disclose a shared-key recovery apparatus, a method used in a shared-key recovery apparatus, and a program embodied on a computer readable storage medium and used in a shared-key recovery apparatus that receives a shared key from a shared-key generation apparatus in secrecy, the shared-key generation apparatus generating a seed value, generating a blind value and a shared key from the seed value, encrypting the seed value based on the blind value to generate encryption information, and transmitting the encryption information, comprising,

- "a receiving unit operable to receive the encryption information" (i.e. "Optional Transmission of S or K: If needed, SKR can transmit either or both S and K") [column 19 lines 3-4];

- "a shared-key generating unit operable to generate a decryption blind value and a decryption shared key, using the decryption seed value and according to a same shared-key generating method used in the shared-key generation apparatus" (i.e. "Alice derives from S a value KG for each agent, by hashing S and the respective agent's ID (step 904)") [column 17 lines 29-30];
- "a re-encryption unit operable to encrypt the decryption seed value based on the decryption blind value, to generate re-encryption information" (i.e. "Alice encrypts the KG values under the respective agents' public keys (step 906)… PUa1: public key for Alice's first agent…KGa1: key-generating key for Alice's first agent") [column 17 lines 31,32, 41, & 46];

but, they do not disclose,

- "a decryption unit operable to decrypt the encryption information, to generate a decryption seed value," although Gennaro-618 do suggest a hash, as recited below;
- "a judging unit operable to judge, based on the encryption information and the reencryption information, whether the decryption shared key should be outputted," although Gennaro-618 do suggest verification based on at least one hash, as recited below;
- "an outputting unit operable, when the judging unit has judged affirmatively, to output the decryption shared key," although Gennaro-618 do suggest verification, as recited below;

however, Gennaro-618 do disclose,

- from Alice (step 1002), Bob locates the previously cached values KGa1-KGb2, using the hash value Hash(B1) in the block B2 as an index (step 1004)" [column 14 lines 3-5];
- "if there are multiple sets of key recovery agents as in the present example, then Bob must ensure that all of the various versions of K agree if he is to fully validate the recovery information" [column 14 lines 25-28];
- "As disclosed in the copending Gennaro et al. application, the decryption procedure 1200 may be keyed to the receiver verification steps so that the message is not decrypted unless all or a specified subset of the key recovery fields in data block B1 and B2 have been verified" [column 14 lines 51-56];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "a decryption unit operable to decrypt the encryption information, to generate a decryption seed value" and "a judging unit operable to judge, based on the encryption information and the reencryption information, whether the decryption shared key should be outputted" and "an outputting unit operable, when the judging unit has judged affirmatively, to output the decryption shared key," in the invention as disclosed by Gennaro-066 since it is reasonable to expect that Gennaro et al. would combine elements from both of his own inventions for the purposes of decryption and verification.

6. Claims 2 & 22-37 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gennaro et al. (US-5937066-A) herein known as Gennaro-066 in view of Gennaro et al. (US-5907618-A) herein known as Gennaro-618 and in further view of Hoffstein et al. (WO-9808323-A1).

Claim 2:

Gennaro-066 and Gennaro-618 disclose a key agreement system comprising a shared-key generation apparatus and a shared-key recovery apparatus, each apparatus establishing therein a same shared key in secrecy, as in Claim 1 above, but their combination do not disclose,

- "the shared-key generation apparatus further includes: an obtaining unit operable to obtain a content," although Hoffstein et al. do suggest reception of information, as recited below;
- "an encryption unit operable to encrypt the obtained content using the shared key, to generate an encrypted content," although Hoffstein et al. do suggest public key encryption, as recited below;
- "the transmitting unit further transmits the encrypted content," although Hoffstein et al. do suggest communicating encrypted data/information, as recited below;
- "the receiving unit further receives the encrypted content," although Hoffstein et al. do suggest receiving encrypted data/information, as recited below;
- "the shared-key recovery apparatus further includes: a decryption unit operable to decrypt the received encrypted content using the decryption shared key, to generate a decrypted content," although Hoffstein et al. do suggest decryption of data/information, as recited below;

- "an outputting unit operable to output the decrypted content," although Hoffstein et al. do suggest decrypting and outputting data/information, as recited below;

however, Hoffstein et al. do disclose,

- [Fig 4 Box# 420 illustrates obtaining data/information];
- "The encoding technique of an embodiment of the public key cryptosystem hereof uses a mixing system based on polynomial algebra and reduction modulo two numbers, p and q, while the decoding technique uses an unmixing system whose validity depends on the elementary probability theory" [page 9];
- "Communication is via transceiver…" [page 8 lines 22-24];
- [Fig 5 Box# 530 illustrates receiving encrypted data/information];
- "The decoding for this matrix example is described next…Finally Dan computes…to recover the original message m" [page 20];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "the shared-key generation apparatus further includes: an obtaining unit operable to obtain a content" and "an encryption unit operable to encrypt the obtained content using the shared key, to generate an encrypted content" and "the transmitting unit further transmits the encrypted content" and "the receiving unit further receives the encrypted content" and "the shared-key recovery apparatus further includes: a decryption unit operable to decrypt the received encrypted content using the decryption shared key, to generate a decrypted content" and "an outputting unit operable to output the decrypted content," in the invention as disclosed by Gennaro-066 and Gennaro-618 for the purposes of the encryption/decryption of data according to a NTRU cryptosystem using public keys.

Claims 22 & 23:

Gennaro-066 and Gennaro-618 disclose a shared-key recovery apparatus that receives a shared key from a shared-key generation apparatus in secrecy, the shared-key generation apparatus generating a seed value, generating a blind value and a shared key from the seed value, encrypting the seed value based on the blind value to generate encryption information, and transmitting the encryption information, as in Claim 21, above, but their combination do not disclose,

- "the shared-key generation apparatus performs a one-way function on the seed value to generate a functional value, generates the blind value and the shared key from the functional value, obtains a public key, performs a public-key encryption algorithm on the seed value using the public key and the blind value, to generate an encryption seed value as the encryption information, and transmits the encryption seed value," although Hoffstein et al. do suggest the usage of polynomials and hashing in a public/private key encryption scheme, as recited below;
- "the receiving unit receives the encryption seed value as the encryption information," although Hoffstein et al. do suggest the usage of polynomials and hashing in a public/private key encryption scheme, as recited below;
- "the decryption unit includes: a secret-key obtaining subunit operable to obtain a secret key that corresponds to the public key," although Hoffstein et al. do suggest the usage of polynomials and hashing in a public/private key encryption scheme, as recited below;

- "a public-key decryption subunit operable to perform, on the received encryption seed value, a public-key decryption algorithm that corresponds to the public-key encryption algorithm, using the obtained secret key, to generate the decryption seed value," although Hoffstein et al. do suggest the usage of polynomials and hashing in a public/private key encryption scheme, as recited below;
- "the shared-key generating unit performs the one-way function on the decryption seed value to generate a decryption functional value, and generates the decryption blind value and the decryption shared key from the decryption functional value," although Hoffstein et al. do suggest the usage of polynomials and hashing in a public/private key encryption scheme, as recited below;
- "the re-encryption unit includes: a public-key obtaining subunit operable to obtain the public key," although Hoffstein et al. do suggest the usage of polynomials and hashing in a public/private key encryption scheme, as recited below;
- "a re-encryption subunit operable to perform the public-key encryption algorithm on the decryption seed value using the public key and the decryption blind value, to generate a reencryption seed value as the re-encryption information," although Hoffstein et al. do suggest the usage of polynomials and hashing in a public/private key encryption scheme, as recited below;
- "the judging unit judges whether the encryption seed value is identical to the re-encryption seed value, and when judging affirmatively, determines that the decryption shared key should be outputted," although Hoffstein et al. do suggest the usage of polynomials and hashing in a public/private key encryption scheme, as recited below;

- "the public-key encryption algorithm and the public-key decryption algorithm conform to an NTRU cryptosystem," although Hoffstein et al. do suggest the usage of polynomials and hashing in a public/private key encryption scheme, as recited below;
- "the shared-key generation apparatus obtains a public-key polynomial generated according to a key-generation algorithm of the NTRU. cryptosystem, as the public key, generates a seed-value polynomial from the seed value, generates a blind-value polynomial from the blind value, encrypts the seed-value polynomial according to an encryption algorithm of the NTRU cryptosystem, using the public-key polynomial as a key, and using the blind-value polynomial to randomize the seed-value polynomial, to generate an encryption seed-value polynomial as the encryption seed value, and transmits the encryption seed-value polynomial as the encryption seed value," although Hoffstein et al. do suggest the usage of polynomials and hashing in a public/private key encryption scheme and NTRU, as recited below;
- "the receiving unit receives the encryption seed-value polynomial as the encryption seed value," although Hoffstein et al. do suggest the usage of polynomials and hashing in a public/private key encryption scheme, as recited below;
- "the secret-key obtaining subunit obtains a secret-key polynomial generated according to the key-generation algorithm of the NTRU cryptosystem, as the secret key," although Hoffstein et al. do suggest the usage of polynomials and hashing in a public/private key encryption scheme and NTRU, as recited below;

- "the public-key decryption subunit decrypts the received encryption seed-value polynomial according to a decryption algorithm of the NTRU cryptosystem and using the obtained secret-key polynomial as a key, to generate a decryption seed-value polynomial, and generates the decryption seed value from the decryption seed-value polynomial," although Hoffstein et al. do suggest the usage of polynomials and hashing in a public/private key encryption scheme, as recited below;
- "the public-key obtaining subunit obtains the public-key polynomial as the public key," although Hoffstein et al. do suggest the usage of polynomials and hashing in a public/private key encryption scheme, as recited below;
- "the re-encryption subunit generates a seed-value polynomial from the decryption seed value, generates a blind-value polynomial from the decryption blind value, and encrypts the seedvalue polynomial according to the encryption algorithm of the NTRU cryptosystem, using the public-key polynomial as a key, and using the blind-value polynomial to randomize the seedvalue polynomial, to generate a re-encryption seed-value polynomial," although Hoffstein et al. do suggest the usage of polynomials and hashing in a public/private key encryption scheme and NTRU, as recited below;
- "the judging unit judges whether the encryption seed-value polynomial is identical to the re-encryption seed-value polynomial," although Hoffstein et al. do suggest the usage of polynomials and hashing in a public/private key encryption scheme, as recited below;

however, Hoffstein et al. do disclose,

- "1.2 Key Creation. To create an NTRU key…1.3 Encoding…Dan randomly chooses…The polynomial f must satisfy the additional requirement… Dan next computes the quantities… Dan's public key is the list of polynomials… Dan's private key is the single polynomial f…" [page 31];
- [Fig 5 Box# 530 illustrates receiving encrypted data/information];
- "The public key information can be published; that is, made available to any member of
- the public or to any desired group…" [page 22 lines 12-23];
- "She uses this randomly chosen polynomial Θ, Dan's public key h, and her plaintext message m to create the encoded message e using the formula…" [page 16-17];
- "The decoding for this matrix example is described next…Finally Dan computes…to recover the original message m" [page 20];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "the shared-key generation apparatus performs a one-way function on the seed value to generate a functional value, generates the blind value and the shared key from the functional value, obtains a public key, performs a public-key encryption algorithm on the seed value using the public key and the blind value, to generate an encryption seed value as the encryption information, and transmits the encryption seed value" and "the receiving unit receives the encryption seed value as the encryption information" and "the decryption unit includes: a secret-key obtaining subunit operable to obtain a secret key that corresponds to the public key" and "a public-key decryption subunit operable to perform, on the received encryption seed value, a public-key decryption algorithm that corresponds to the public-

key encryption algorithm, using the obtained secret key, to generate the decryption seed value" and "the shared-key generating unit performs the one-way function on the decryption seed value to generate a decryption functional value, and generates the decryption blind value and the decryption shared key from the decryption functional value" and "the re-encryption unit includes: a public-key obtaining subunit operable to obtain the public key" and "a re-encryption subunit operable to perform the public-key encryption algorithm on the decryption seed value using the public key and the decryption blind value, to generate a reencryption seed value as the re-encryption information" and "the judging unit judges whether the encryption seed value is identical to the re-encryption seed value, and when judging affirmatively, determines that the decryption shared key should be outputted" and "the public-key encryption algorithm and the public-key decryption algorithm conform to an NTRU cryptosystem" and "the shared-key generation apparatus obtains a public-key polynomial generated according to a key-generation algorithm of the NTRU. cryptosystem, as the public key, generates a seed-value polynomial from the seed value, generates a blind-value polynomial from the blind value, encrypts the seed-value polynomial according to an encryption algorithm of the NTRU cryptosystem, using the public-key polynomial as a key, and using the blind-value polynomial to randomize the seed-value polynomial, to generate an encryption seed-value polynomial as the encryption seed value, and transmits the encryption seed-value polynomial as the encryption seed value" and "the receiving unit receives the encryption seed-value polynomial as the encryption seed value" and "the secret-key obtaining subunit obtains a secret-key polynomial generated according to the key-generation algorithm of the NTRU cryptosystem, as the secret key" and "the public-key decryption subunit decrypts the received encryption seed-value polynomial according to a decryption algorithm of

the NTRU cryptosystem and using the obtained secret-key polynomial as a key, to generate a decryption seed-value polynomial, and generates the decryption seed value from the decryption seed-value polynomial" and "the public-key obtaining subunit obtains the public-key polynomial as the public key" and "the re-encryption subunit generates a seed-value polynomial from the decryption seed value, generates a blind-value polynomial from the decryption blind value, and encrypts the seedvalue polynomial according to the encryption algorithm of the NTRU cryptosystem, using the public-key polynomial as a key, and using the blind-value polynomial to randomize the seedvalue polynomial, to generate a re-encryption seed-value polynomial" and "the judging unit judges whether the encryption seed-value polynomial is identical to the re-encryption seed-value polynomial," in the invention as disclosed by Gennaro-066 and Gennaro-618 for the purposes of the encryption/decryption of data according to a NTRU cryptosystem using public keys.

Claims 24-27:

Gennaro-066 and Gennaro-618 disclose a shared-key recovery apparatus that receives a shared key from a shared-key generation apparatus in secrecy, the shared-key generation apparatus generating a seed value, generating a blind value and a shared key from the seed value, encrypting the seed value based on the blind value to generate encryption information, and transmitting the encryption information, as in Claim 21, above, but their combination do not disclose,

- "wherein the shared-key generation apparatus obtains a public key, generates a blind value, performs a public-key encryption algorithm on the seed value using the public key and the blind value to generate a public-key cipher text, performs a second one-way

function on at least one of the seed value, the blind value, and the shared key to generate a second functional value, generates the encryption information that includes the public-key cipher text and the second functional value, and transmits the encryption information," although Hoffstein et al. do suggest the usage of polynomials and hashing in a public/private key encryption scheme, as recited below;

- "the receiving unit receives the encryption information that includes the public-key cipher text and the second functional value," although Hoffstein et al. do suggest the usage of polynomials and hashing in a public/private key encryption scheme, as recited below;
- "the decryption unit includes: a secret-key obtaining subunit operable to obtain a secret key that corresponds to the public key," although Hoffstein et al. do suggest the usage of polynomials and hashing in a public/private key encryption scheme, as recited below;
- "a public-key decryption subunit operable to perform, on the public-key cipher text included in the received encryption information, a public-key decryption algorithm that corresponds to the public-key encryption algorithm, to generate a decryption seed value," although Hoffstein et al. do suggest the usage of polynomials and hashing in a public/private key encryption scheme, as recited below;
- "a function subunit operable to perform the second one-way function on at least one of the decryption seed value, the decryption blind value, and the decryption shared key, to generate a decryption second functional value," although Hoffstein et al. do suggest the usage of polynomials and hashing in a public/private key encryption scheme, as recited below;

- "the judging unit judges whether the second functional value included in the received encryption information is identical to the decryption second functional value instead of performing judging based on the encryption information and the re-encryption information, and when judging affirmatively, determines that the decryption shared key should be outputted," although Hoffstein et al. do suggest the usage of polynomials and hashing in a public/private key encryption scheme, as recited below;
- "wherein the shared-key generation apparatus performs a one-way function on the seed value to generate a functional value, and generates the blind value and the shared key from the functional value," although Hoffstein et al. do suggest the usage of polynomials and hashing in a public/private key encryption scheme, as recited below;
- "the shared-key generating unit performs the first one-way function on the decryption seed value to generate a decryption functional value, and generates the decryption blind value and the decryption shared key from the decryption functional value," although Hoffstein et al. do suggest the usage of polynomials and hashing in a public/private key encryption scheme, as recited below;
- "wherein the shared-key generation apparatus performs a first one-way function on the seed value to generate a first functional value, and generates the shared key from the first functional value, instead of generating the blind value and the shared key," although Hoffstein et al. do suggest the usage of polynomials and hashing in a public/private key encryption scheme, as recited below;

- "the shared-key generating unit performs the first one-way function on the decryption seed value to generate a decryption functional value, and generates the decryption shared key from the decryption functional value, instead of generating the decryption blind value and the decryption shared key," although Hoffstein et al. do suggest the usage of polynomials and hashing in a public/private key encryption scheme and NTRU, as recited below;
- "wherein the public-key encryption algorithm and the public-key decryption algorithm conform to an NTRU cryptosystem," although Hoffstein et al. do suggest the usage of polynomials and hashing in a public/private key encryption scheme, as recited below;
- "the shared-key generation apparatus obtains a public-key polynomial generated according to a key-generation algorithm of the NTRU cryptosystem, as the public key, generates a seed-value polynomial from the seed value, generates a blind-value polynomial from the blindvalue, encrypts the seed-value polynomial according to an encryption algorithm of the NTRU cryptosystem using the public-key polynomial as a key and using the blind-value polynomial to randomize the seed-value polynomial, to generate an encryption seed-value polynomial as the public-key cipher text, and generates the encryption information that includes the encryption seed-value polynomial as the public-key cipher text and the second functional value," although Hoffstein et al. do suggest the usage of polynomials and hashing in a public/private key encryption scheme and NTRU, as recited below;

- "the secret-key obtaining subunit obtains a secret-key polynomial generated according to the key-generation algorithm of the NTRU cryptosystem, as the secret key," although Hoffstein et al. do suggest the usage of polynomials and hashing in a public/private key encryption scheme, as recited below;
- "the public-key decryption subunit generates a public-key cipher-text polynomial from the public-key cipher text, decrypts the public-key cipher-text polynomial according to a decryption algorithm of the NTRU cryptosystem using the secret-key polynomial as a key to generate a decryption seed-value polynomial, and generates the decryption seed value from the decryption seed-value polynomial," although Hoffstein et al. do suggest the usage of polynomials and hashing in a public/private key encryption scheme, as recited below;

however, Hoffstein et al. do disclose,

- "1.2 Key Creation. To create an NTRU key…1.3 Encoding…Dan randomly chooses…The polynomial f must satisfy the additional requirement… Dan next computes the quantities… Dan's public key is the list of polynomials… Dan's private key is the single polynomial f…" [page 31];
- "She uses this randomly chosen polynomial Θ, Dan's public key h, and her plaintext message m to create the encoded message e using the formula…" [page 16-17];
- "The decoding for this matrix example is described next…Finally Dan computes…to recover the original message m" [page 20];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "wherein the shared-key generation apparatus obtains a public key, generates a blind value, performs a public-key encryption algorithm on the seed value using the public key and the blind value to generate a public-key cipher text, performs a second one-way function on at least one of the seed value, the blind value, and the shared key to generate a second functional value, generates the encryption information that includes the public-key cipher text and the second functional value, and transmits the encryption information" and "the receiving unit receives the encryption information that includes the public-key cipher text and the second functional value" and "the decryption unit includes: a secret-key obtaining subunit operable to obtain a secret key that corresponds to the public key" and "a public-key decryption subunit operable to perform, on the public-key cipher text included in the received encryption information, a public-key decryption algorithm that corresponds to the public-key encryption algorithm, to generate a decryption seed value" and "a function subunit operable to perform the second one-way function on at least one of the decryption seed value, the decryption blind value, and the decryption shared key, to generate a decryption second functional value" and "the judging unit judges whether the second functional value included in the received encryption information is identical to the decryption second functional value instead of performing judging based on the encryption information and the re-encryption information, and when judging affirmatively, determines that the decryption shared key should be outputted" and "wherein the shared-key generation apparatus performs a one-way function on the seed value to generate a functional value, and generates the blind value and the shared key from the functional value" and "the shared-key generating unit performs the first one-way function on the decryption seed value

to generate a decryption functional value, and generates the decryption blind value and the decryption shared key from the decryption functional value" and "wherein the shared-key generation apparatus performs a first one-way function on the seed value to generate a first functional value, and generates the shared key from the first functional value, instead of generating the blind value and the shared key" and "the shared-key generating unit performs the first one-way function on the decryption seed value to generate a decryption functional value, and generates the decryption shared key from the decryption functional value, instead of generating the decryption blind value and the decryption shared key" and "wherein the public-key encryption algorithm and the public-key decryption algorithm conform to an NTRU cryptosystem" and "the shared-key generation apparatus obtains a public-key polynomial generated according to a key-generation algorithm of the NTRU cryptosystem, as the public key, generates a seed-value polynomial from the seed value, generates a blind-value polynomial from the blindvalue, encrypts the seed-value polynomial according to an encryption algorithm of the NTRU cryptosystem using the public-key polynomial as a key and using the blind-value polynomial to randomize the seed-value polynomial, to generate an encryption seed-value polynomial as the public-key cipher text, and generates the encryption information that includes the encryption seed-value polynomial as the public-key cipher text and the second functional value" and "the secret-key obtaining subunit obtains a secret-key polynomial generated according to the key-generation algorithm of the NTRU cryptosystem, as the secret key" and "the public-key decryption subunit generates a public-key cipher-text polynomial from the public-key cipher text, decrypts the public-key cipher-text polynomial according to a decryption algorithm of the NTRU cryptosystem using the secret-key polynomial as a key to generate a

decryption seed-value polynomial, and generates the decryption seed value from the decryption seed-value polynomial," in the invention as disclosed by Gennaro-066 and Gennaro-618 for the purposes of the encryption/decryption of data according to a NTRU cryptosystem using public keys.

Claims 29-33:

Gennaro-066 and Gennaro-618 disclose a shared-key recovery apparatus that receives a shared key from a shared-key generation apparatus in secrecy, the shared-key generation apparatus generating a seed value, generating a blind value and a shared key from the seed value, encrypting the seed value based on the blind value to generate encryption information, and transmitting the encryption information, as in Claim 21, above, but their combination do not disclose,

- "the shared-key generation apparatus performs a one-way function on the seed value to generate a functional value, generates a verification value, the blind value, and the shared key from the functional value, obtains a public key, performs a public-key encryption algorithm on the verification value using the public key and the blind value to generate a first cipher text, performs, based on the verification value, a computation algorithm different from the public-key encryption algorithm on the seed value, to generate a second cipher text, generates the encryption information that includes the first cipher text and the second cipher text, and transmits the encryption information," although Hoffstein et al. do suggest the usage of polynomials and hashing in a public/private key encryption scheme, as recited below;

- "the receiving unit receives the encryption information that includes the first cipher text and the second cipher text," although Hoffstein et al. do suggest the usage of polynomials and hashing in a public/private key encryption scheme, as recited below;
- "the decryption unit includes: a secret-key obtaining subunit operable to obtain a secret key that corresponds to the public key," although Hoffstein et al. do suggest the usage of polynomials and hashing in a public/private key encryption scheme, as recited below;
- "a public-key decryption subunit operable to perform, on the first cipher text included in the received encryption information, a public-key decryption algorithm that corresponds to the public-key encryption algorithm, to generate a decryption verification value," although Hoffstein et al. do suggest the usage of polynomials and hashing in a public/private key encryption scheme, as recited below;
- "a computation decryption subunit operable to perform, on the second cipher text included in the received encryption information, a computation algorithm for performing an inverse computation of the different computation algorithm, to generate a decryption seed value," although Hoffstein et al. do suggest the usage of polynomials and hashing in a public/private key encryption scheme, as recited below;
- "the shared-key generating unit performs the one-way function on the decryption seed value to generate a decryption functional value, and generates a decryption verification value, the decryption blind value, and the decryption shared key, from the decryption functional value," although Hoffstein et al. do suggest the usage of polynomials and hashing in a public/private key encryption scheme, as recited below;

- "the re-encryption unit includes: a public-key obtaining subunit operable to obtain the public key," although Hoffstein et al. do suggest the usage of polynomials and hashing in a public/private key encryption scheme, as recited below;
- "a re-encryption subunit operable to perform, on the decryption verification value, the public-key encryption algorithm using the public key and the decryption blind value, to generate the re-encryption information," although Hoffstein et al. do suggest the usage of polynomials and hashing in a public/private key encryption scheme, as recited below;
- "the judging unit judges whether the first cipher text included in the encryption information is identical to the re-encryption information, and when judging affirmatively, determines that the decryption shared key should be outputted," although Hoffstein et al. do suggest the usage of polynomials and hashing in a public/private key encryption scheme, as recited below;
- "wherein the public-key encryption algorithm and the public-key decryption algorithm conform to an NTRU cryptosystem," although Hoffstein et al. do suggest the usage of polynomials and hashing in a public/private key encryption scheme and NTRU, as recited below;
- "the shared-key generation apparatus obtains a public-key polynomial generated according to a key-generation algorithm of the NTRU cryptosystem, as the public key, generates a verification-value polynomial from the verification value, generates a blind-value polynomial from the blind value, encrypts the verification-value polynomial according to an encryption algorithm of the NTRU cryptosystem, using the public-key polynomial as a key, and using the blind-value polynomial to randomize the verification-

value polynomial, to generate an encryption verification-value polynomial as the first cipher text, generates the encryption information that includes the encryption verification-value polynomial as the first cipher text and the second cipher text, and transmits the encryption information," although Hoffstein et al. do suggest the usage of polynomials and hashing in a public/private key encryption scheme and NTRU, as recited below;

- "the receiving unit receives the encryption information that includes the encryption verification-value polynomial and the second cipher text," although Hoffstein et al. do suggest the usage of polynomials and hashing in a public/private key encryption scheme and NTRU, as recited below;
- "the secret-key obtaining subunit obtains a secret-key polynomial generated according to the key-generation algorithm of the NTRU cryptosystem, as the secret key," although Hoffstein et al. do suggest the usage of polynomials and hashing in a public/private key encryption scheme and NTRU, as recited below;
- "the public-key decryption subunit generates a first cipher-text polynomial from the first cipher text, decrypts the first cipher-text polynomial according to a decryption algorithm of the NTRU cryptosystem using the secret-key polynomial as a key, to generate a decryption verification polynomial, and generates the decryption verification value from the decryption verification-value polynomial," although Hoffstein et al. do suggest the usage of polynomials and hashing in a public/private key encryption scheme and NTRU, as recited below;

- "the public-key obtaining subunit obtains the public-key polynomial," although Hoffstein et al. do suggest the usage of polynomials and hashing in a public/private key encryption scheme and NTRU, as recited below;
- "the re-encryption subunit generates a decryption verification-value polynomial from the decryption verification value, generates a blind-value polynomial from the decryption blind value, and encrypts the decryption verification-value polynomial according to the encryption algorithm of the NTRU cryptosystem, using the public-key polynomial as a key, and using the blind-value polynomial to randomize the decryption verification-value polynomial, to generate a re-encryption verification-value polynomial as the re-encryption information," although Hoffstein et al. do suggest the usage of polynomials and hashing in a public/private key encryption scheme and NTRU, as recited below;
- "the judging unit judges whether the encryption verification-value polynomial as the first cipher text is identical to the re-encryption verification-value polynomial as the re-encryption information," although Hoffstein et al. do suggest the usage of polynomials and hashing in a public/private key encryption scheme and NTRU, as recited below;
- "wherein the different computation algorithm is a symmetric key encryption algorithm, and the computation algorithm for performing the inverse computation is a corresponding symmetric key decryption algorithm," although Hoffstein et al. do suggest the usage of polynomials and hashing in a public/private key encryption scheme, as recited below;

- "the computation decryption subunit performs the symmetric key decryption algorithm on the second cipher text, using the decryption verification value as a key, to generate the decryption seed value," although Hoffstein et al. do suggest the usage of polynomials and hashing in a public/private key encryption scheme, as recited below;
- "the different computation algorithm and the computation algorithm for performing the inverse computation are bitwise exclusive-or," although Hoffstein et al. do suggest the usage of polynomials and hashing in a public/private key encryption scheme, as recited below;
- "the computation decryption subunit performs the bitwise exclusive-or on the decryption verification value and the second cipher text, to generate the decryption seed value," although Hoffstein et al. do suggest the usage of polynomials and hashing in a public/private key encryption scheme, as recited below;
- "wherein the different computation algorithm is addition and the computation algorithm for performing the inverse computation is subtraction," although Hoffstein et al. do suggest the usage of polynomials and hashing in a public/private key encryption scheme, as recited below;
- "the computation decryption subunit performs the subtraction on the decryption verification value and the second cipher text, to generate the decryption seed value," although Hoffstein et al. do suggest the usage of polynomials and hashing in a public/private key encryption scheme, as recited below;

- "wherein the different calculation algorithm is multiplication and the computation algorithm for performing the inverse computation is division," although Hoffstein et al. do suggest the usage of polynomials and hashing in a public/private key encryption scheme, as recited below;
- "the computation decryption subunit performs the division on the decryption verification value and the second cipher text, to generate the decryption seed value," although Hoffstein et al. do suggest the usage of polynomials and hashing in a public/private key encryption scheme, as recited below;

however, Hoffstein et al. do disclose,

- "1.2 Key Creation. To create an NTRU key…1.3 Encoding…Dan randomly chooses…The polynomial f must satisfy the additional requirement… Dan next computes the quantities… Dan's public key is the list of polynomials… Dan's private key is the single polynomial f…" [page 31];
- "She uses this randomly chosen polynomial Θ, Dan's public key h, and her plaintext message m to create the encoded message e using the formula…" [page 16-17];
- "The decoding for this matrix example is described next…Finally Dan computes…to recover the original message m" [page 20];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "the shared-key generation apparatus performs a one-way function on the seed value to generate a functional value, generates a verification value, the blind value, and the shared key from the functional value, obtains a public key, performs a public-key encryption algorithm on the verification value using the public key and the blind value to

generate a first cipher text, performs, based on the verification value, a computation algorithm different from the public-key encryption algorithm on the seed value, to generate a second cipher text, generates the encryption information that includes the first cipher text and the second cipher text, and transmits the encryption information" and "the receiving unit receives the encryption information that includes the first cipher text and the second cipher text" and "the decryption unit includes: a secret-key obtaining subunit operable to obtain a secret key that corresponds to the public key" and "a public-key decryption subunit operable to perform, on the first cipher text included in the received encryption information, a public-key decryption algorithm that corresponds to the public-key encryption algorithm, to generate a decryption verification value" and "a computation decryption subunit operable to perform, on the second cipher text included in the received encryption information, a computation algorithm for performing an inverse computation of the different computation algorithm, to generate a decryption seed value" and "the shared-key generating unit performs the one-way function on the decryption seed value to generate a decryption functional value, and generates a decryption verification value, the decryption blind value, and the decryption shared key, from the decryption functional value" and "the re-encryption unit includes: a public-key obtaining subunit operable to obtain the public key" and "a re-encryption subunit operable to perform, on the decryption verification value, the public-key encryption algorithm using the public key and the decryption blind value, to generate the re-encryption information" and "the judging unit judges whether the first cipher text included in the encryption information is identical to the re-encryption information, and when judging affirmatively, determines that the decryption shared key should be outputted" and "wherein the public-key encryption algorithm and the public-key decryption algorithm conform to an NTRU

cryptosystem" and "the shared-key generation apparatus obtains a public-key polynomial generated according to a key-generation algorithm of the NTRU cryptosystem, as the public key, generates a verification-value polynomial from the verification value, generates a blind-value polynomial from the blind value, encrypts the verification-value polynomial according to an encryption algorithm of the NTRU cryptosystem, using the public-key polynomial as a key, and using the blind-value polynomial to randomize the verification-value polynomial, to generate an encryption verification-value polynomial as the first cipher text, generates the encryption information that includes the encryption verification-value polynomial as the first cipher text and the second cipher text, and transmits the encryption information" and "the receiving unit receives the encryption information that includes the encryption verification-value polynomial and the second cipher text" and "the secret-key obtaining subunit obtains a secret-key polynomial generated according to the key-generation algorithm of the NTRU cryptosystem, as the secret key" and "the public-key decryption subunit generates a first cipher-text polynomial from the first cipher text, decrypts the first cipher-text polynomial according to a decryption algorithm of the NTRU cryptosystem using the secret-key polynomial as a key, to generate a decryption verification polynomial, and generates the decryption verification value from the decryption verification-value polynomial" and "the public-key obtaining subunit obtains the public-key polynomial" and "the re-encryption subunit generates a decryption verification-value polynomial from the decryption verification value, generates a blind-value polynomial from the decryption blind value, and encrypts the decryption verification-value polynomial according to the encryption algorithm of the NTRU cryptosystem, using the public-key polynomial as a key, and using the blind-value polynomial to randomize the decryption verification-value polynomial, to

generate a re-encryption verification-value polynomial as the re-encryption information" and "the judging unit judges whether the encryption verification-value polynomial as the first cipher text is identical to the re-encryption verification-value polynomial as the re-encryption information" and "wherein the different computation algorithm is a symmetric key encryption algorithm, and the computation algorithm for performing the inverse computation is a corresponding symmetric key decryption algorithm" and "the computation decryption subunit performs the symmetric key decryption algorithm on the second cipher text, using the decryption verification value as a key, to generate the decryption seed value" and "the different computation algorithm and the computation algorithm for performing the inverse computation are bitwise exclusive-or" and "the computation decryption subunit performs the bitwise exclusive-or on the decryption verification value and the second cipher text, to generate the decryption seed value" and "wherein the different computation algorithm is addition and the computation algorithm for performing the inverse computation is subtraction" and "the computation decryption subunit performs the subtraction on the decryption verification value and the second cipher text, to generate the decryption seed value" and "wherein the different calculation algorithm is multiplication and the computation algorithm for performing the inverse computation is division" and "the computation decryption subunit performs the division on the decryption verification value and the second cipher text, to generate the decryption seed value," in the invention as disclosed by Gennaro-066 and Gennaro-618 for the purposes of the encryption/decryption of data according to a NTRU cryptosystem using public keys.

Claims 34-36:

Gennaro-066 and Gennaro-618 disclose a shared-key recovery apparatus that receives a shared key from a shared-key generation apparatus in secrecy, the shared-key generation apparatus generating a seed value, generating a blind value and a shared key from the seed value, encrypting the seed value based on the blind value to generate encryption information, and transmitting the encryption information, as in Claim 21, above, but their combination do not disclose,

- "wherein the shared-key generating unit performs a one-way function on the decryption seed value to generate a functional value, and generates the decryption blind value and the decryption shared key from the functional value," although Hoffstein et al. do suggest the usage of polynomials and hashing in a public/private key encryption scheme, as recited below;
- "wherein the one-way function is a hash function, and the shared-key generating unit performs the hash function on the decryption seed value," although Hoffstein et al. do suggest the usage of polynomials and hashing in a public/private key encryption scheme, as recited below;
- "wherein the shared-key generating unit generates the decryption blind value by setting a part of the functional value as the decryption blind value, and generates the decryption shared key by setting another part of the functional value as the decryption shared key," although Hoffstein et al. do suggest the usage of polynomials and hashing in a public/private key encryption scheme, as recited below;

however, Hoffstein et al. do disclose,

- "She uses this randomly chosen polynomial Θ, Dan's public key h, and her plaintext message m to create the encoded message e using the formula…" [page 16-17];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "wherein the shared-key generating unit performs a one-way function on the decryption seed value to generate a functional value, and generates the decryption blind value and the decryption shared key from the functional value" and "wherein the one-way function is a hash function, and the shared-key generating unit performs the hash function on the decryption seed value" and "wherein the shared-key generating unit generates the decryption blind value by setting a part of the functional value as the decryption blind value, and generates the decryption shared key by setting another part of the functional value as the decryption shared key," in the invention as disclosed by Gennaro-066 and Gennaro-618 for the purposes of the encryption/decryption of data according to a NTRU cryptosystem using public keys..

Claim 37:

Gennaro-066 and Gennaro-618 disclose a shared-key recovery apparatus that receives a shared key from a shared-key generation apparatus in secrecy, the shared-key generation apparatus generating a seed value, generating a blind value and a shared key from the seed value, encrypting the seed value based on the blind value to generate encryption information, and transmitting the encryption information, as in Claim 21, above, but their combination do not disclose,

- "wherein the shared-key generation apparatus further obtains a content, encrypts the obtained content using the shared key to generate an encrypted content, and transmits the encrypted content," although Hoffstein et al. do suggest the usage of polynomials and hashing in a public/private key encryption scheme, as recited below;
- "the shared-key recovery apparatus further includes: a content receiving unit operable to receive the encrypted content," although Hoffstein et al. do suggest the usage of polynomials and hashing in a public/private key encryption scheme, as recited below;
- "a decryption unit operable to decrypt the received encrypted content using the outputted decryption shared key, to generate a decrypted content," although Hoffstein et al. do suggest the usage of polynomials and hashing in a public/private key encryption scheme, as recited below;
- "a playback unit operable to playback the decrypted content," although Hoffstein et al. do suggest the usage of polynomials and hashing in a public/private key encryption scheme, as recited below;

however, Hoffstein et al. do disclose,

- "She uses this randomly chosen polynomial Θ, Dan's public key h, and her plaintext message m to create the encoded message e using the formula..." [page 16-17];
- [Fig 5 Box# 530 illustrates receiving encrypted data/information];
- "The decoding for this matrix example is described next...Finally Dan computes...to recover the original message m" [page 20];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "wherein the shared-key generation apparatus further obtains a content, encrypts the obtained content using the shared key to generate an encrypted content, and transmits the encrypted content" and "the shared-key recovery apparatus further includes: a content receiving unit operable to receive the encrypted content" and "a decryption unit operable to decrypt the received encrypted content using the outputted decryption shared key, to generate a decrypted content" and "a playback unit operable to playback the decrypted content," in the invention as disclosed by Gennaro-066 and Gennaro-618 for the purposes of the encryption/decryption of data according to a NTRU cryptosystem using public keys.

7. Claims 4-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gennaro et al. (US-5937066-A) herein known as Gennaro-066 in view of Hoffstein et al. (WO-9808323-A1).

Claims 4 & 5:

Gennaro-066 disclose a shared-key generation apparatus that notifies a destination apparatus about a shared key in secrecy, as in Claim 3 above, but do not disclose,

- "wherein the shared-key generating unit performs a one-way function on the seed value, to generate a functional value, and generates the blind value and the shared key from the functional value," although Hoffstein et al. do suggest the usage of polynomials and hashing in a public/private key encryption scheme and NTRU, as recited below;
- "the encryption unit includes: a public-key obtaining subunit operable to obtain a public key," although Hoffstein et al. do suggest the usage of polynomials and hashing in a public/private key encryption scheme and NTRU, as recited below;

- "a public-key encryption subunit operable to perform a public-key encryption algorithm on the seed value, using the public key and the blind value, to generate an encryption seed value as the encryption information," although Hoffstein et al. do suggest the usage of polynomials and hashing in a public/private key encryption scheme and NTRU, as recited below;
- "the public-key encryption algorithm conforms to an NTRU cryptosystem," although Hoffstein et al. do suggest the usage of polynomials and hashing in a public/private key encryption scheme and NTRU, as recited below;
- "the public-key obtaining subunit obtains a public-key polynomial generated according to a key-generation algorithm of the NTRU cryptosystem, as the public key," although Hoffstein et al. do suggest the usage of polynomials and hashing in a public/private key encryption scheme and NTRU, as recited below;
- "the public-key encryption subunit generates a seed-value polynomial from the seed value, generates a blind-value polynomial from the blind value, and encrypts the seed-value polynomial according to an encryption algorithm of the NTRU cryptosystem, using the public key polynomial as a key, and using the blind-value polynomial to randomize the seed-value polynomial, to generate an encryption seed-value polynomial as the encryption seed value," although Hoffstein et al. do suggest the usage of polynomials and hashing in a public/private key encryption scheme and NTRU, as recited below;
- "the transmitting unit transmits the encryption seed-value polynomial as the encryption seed value," although Hoffstein et al. do suggest the usage of polynomials and hashing in a public/private key encryption scheme and NTRU, as recited below;

however, Hoffstein et al. do disclose,

- "She uses this randomly chosen polynomial Θ, Dan's public key h, and her plaintext message m to create the encoded message e using the formula…" [page 16-17];
- "The public key information can be published; that is, made available to any member of the public or to any desired group…" [page 22 lines 12-23];
- "The block 220 represents the routine that can be used by the message sender to encode the plaintext message using the public key of the intended message recipient" [page 22 lines 24-27 & page 23 lines 1-4];
- "1.2 Key Creation. To create an NTRU key…1.3 Encoding…Dan randomly chooses…The polynomial f must satisfy the additional requirement… Dan next computes the quantities… Dan's public key is the list of polynomials… Dan's private key is the single polynomial f…" [page 31];
- "Communication is via transceiver…" [page 8 lines 22-24];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "wherein the shared-key generating unit performs a one-way function on the seed value, to generate a functional value, and generates the blind value and the shared key from the functional value" and "the encryption unit includes: a public-key obtaining subunit operable to obtain a public key" and "a public-key encryption subunit operable to perform a public-key encryption algorithm on the seed value, using the public key and the blind value, to generate an encryption seed value as the encryption information" and "the public-key encryption algorithm conforms to an NTRU cryptosystem" and "the public-key obtaining subunit obtains a public-key polynomial generated according to a key-generation algorithm of

the NTRU cryptosystem, as the public key" and "the public-key encryption subunit generates a seed-value polynomial from the seed value, generates a blind-value polynomial from the blind value, and encrypts the seed-value polynomial according to an encryption algorithm of the NTRU cryptosystem, using the public key polynomial as a key, and using the blind-value polynomial to randomize the seed-value polynomial, to generate an encryption seed-value polynomial as the encryption seed value" and "the transmitting unit transmits the encryption seed-value polynomial as the encryption seed value," in the invention as disclosed by Gennaro-066 for the purposes of the encryption/decryption of data according to a NTRU cryptosystem using public keys.

Claims 6-9:

Gennaro-066 disclose a shared-key generation apparatus that notifies a destination apparatus about a shared key in secrecy, as in Claim 3 above, but do not disclose,

- "a public-key obtaining subunit operable to obtain a public key," although Hoffstein et al. do suggest the usage of polynomials and hashing in a public/private key encryption scheme and NTRU, as recited below;
- "a public-key encryption subunit operable to generate a blind value, perform the public-key encryption algorithm on the seed value using the public key and the blind value, to generate a public-key cipher text," although Hoffstein et al. do suggest the usage of polynomials and hashing in a public/private key encryption scheme and NTRU, as recited below;

- "a function subunit operable to perform a second one-way function on at least one of the seed value, the blind value, and the shared key, to generate a second functional value," although Hoffstein et al. do suggest the usage of polynomials and hashing in a public/private key encryption scheme and NTRU, as recited below;
- "the encryption unit generates the encryption information that includes the public-key cipher text and the second functional value," although Hoffstein et al. do suggest the usage of polynomials and hashing in a public/private key encryption scheme and NTRU, as recited below;
- "the shared-key generating unit performs a one-way function on the seed value, to generate a functional value, and generates the blind value and the shared key from the functional value," although Hoffstein et al. do suggest the usage of polynomials and hashing in a public/private key encryption scheme and NTRU, as recited below;
- "wherein the shared-key generating unit performs a first one-way function on the seed value, to generate a first functional value, and generates the shared key from the first functional value, instead of generating the blind value and the shared key," although Hoffstein et al. do suggest the usage of polynomials and hashing in a public/private key encryption scheme and NTRU, as recited below;
- "the public-key encryption algorithm conforms to an NTRU cryptosystem," although Hoffstein et al. do suggest the usage of polynomials and hashing in a public/private key encryption scheme and NTRU, as recited below;

- "the public-key obtaining subunit obtains a public-key polynomial generated according to a key-generation algorithm of the NTRU cryptosystem, as the public key," although Hoffstein et al. do suggest the usage of polynomials and hashing in a public/private key encryption scheme and NTRU, as recited below;
- "the public-key encryption subunit generates a seed-value polynomial from the seed value, generates a blind-value polynomial from the blind value, encrypts the seed-value polynomial according to an encryption algorithm of the NTRU cryptosystem, using the public key polynomial as a key, and using the blind-value polynomial to randomize the seed-value polynomial, to generate an encryption seed-value polynomial as the public-key cipher text," although Hoffstein et al. do suggest the usage of polynomials and hashing in a public/private key encryption scheme and NTRU, as recited below;
- "the encryption unit generates the encryption information that includes the encryption seed-value polynomial as the public-key cipher text and the second functional value," although Hoffstein et al. do suggest the usage of polynomials and hashing in a public/private key encryption scheme and NTRU, as recited below;

however, Hoffstein et al. do disclose,

- "The public key information can be published; that is, made available to any member of the public or to any desired group…" [page 22 lines 12-23];
- "The block 220 represents the routine that can be used by the message sender to encode the plaintext message using the public key of the intended message recipient" [page 22 lines 24-27 & page 23 lines 1-4];

- "a seed-value generating unit operable to generate a seed value," and, "a shared-key generating unit operable to generate a blind value and a shared key, from the seed value" [pages 13-15];
- "1.2 Key Creation. To create an NTRU key…1.3 Encoding…Dan randomly chooses…The polynomial f must satisfy the additional requirement… Dan next computes the quantities… Dan's public key is the list of polynomials… Dan's private key is the single polynomial f…" [page 31];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "a public-key obtaining subunit operable to obtain a public key" and "a public-key encryption subunit operable to generate a blind value, perform the public-key encryption algorithm on the seed value using the public key and the blind value, to generate a public-key cipher text" and "a function subunit operable to perform a second one-way function on at least one of the seed value, the blind value, and the shared key, to generate a second functional value" and "the encryption unit generates the encryption information that includes the public-key cipher text and the second functional value" and "the shared-key generating unit performs a one-way function on the seed value, to generate a functional value, and generates the blind value and the shared key from the functional value" and "wherein the shared-key generating unit performs a first one-way function on the seed value, to generate a first functional value, and generates the shared key from the first functional value, instead of generating the blind value and the shared key" and "the public-key encryption algorithm conforms to an NTRU cryptosystem" and "the public-key obtaining subunit obtains a public-key polynomial generated according to a key-generation algorithm of the NTRU cryptosystem, as the public key" and "the

public-key encryption subunit generates a seed-value polynomial from the seed value, generates a blind-value polynomial from the blind value, encrypts the seed-value polynomial according to an encryption algorithm of the NTRU cryptosystem, using the public key polynomial as a key, and using the blind-value polynomial to randomize the seed-value polynomial, to generate an encryption seed-value polynomial as the public-key cipher text" and "the encryption unit generates the encryption information that includes the encryption seed-value polynomial as the public-key cipher text and the second functional value," in the invention as disclosed by Gennaro-066 for the purposes of the encryption/decryption of data according to a NTRU cryptosystem using public keys.

Claims 10-15:

Gennaro-066 disclose a shared-key generation apparatus that notifies a destination apparatus about a shared key in secrecy, as in Claim 3 above, but do not disclose,

- "the shared-key generating unit performs a one-way function on the seed value, to generate a functional value, and generates a verification value, the blind value, and the shared key, from the functional value," although Hoffstein et al. do suggest the usage of polynomials and hashing in a public/private key encryption scheme and NTRU, as recited below;
- "the encryption unit includes: a public-key obtaining subunit operable to obtain a public key," although Hoffstein et al. do suggest the usage of polynomials and hashing in a public/private key encryption scheme and NTRU, as recited below;

- "a first encryption subunit operable to perform a public-key encryption algorithm on the verification value, using the public key and the blind value, to generate a first cipher text," although Hoffstein et al. do suggest the usage of polynomials and hashing in a public/private key encryption scheme and NTRU, as recited below;
- "a second encryption subunit operable to perform, on the seed value, a computation algorithm different from the public-key encryption algorithm, to generate a second cipher text," although Hoffstein et al. do suggest the usage of polynomials and hashing in a public/private key encryption scheme and NTRU, as recited below;
- "the encryption unit generates the encryption information that includes the first cipher text and the second cipher text," although Hoffstein et al. do suggest the usage of polynomials and hashing in a public/private key encryption scheme and NTRU, as recited below;
- "the public-key encryption algorithm conforms to an NTRU cryptosystem," although Hoffstein et al. do suggest the usage of polynomials and hashing in a public/private key encryption scheme and NTRU, as recited below;
- "the public-key obtaining subunit obtains a public-key polynomial generated according to a key-generation algorithm of the NTRU cryptosystem, as the public key," although Hoffstein et al. do suggest the usage of polynomials and hashing in a public/private key encryption scheme and NTRU, as recited below;
- "the first encryption subunit generates a verification-value polynomial from the verification value, generates a blind-value polynomial from the blind value, and encrypts the verification-value polynomial according to an encryption algorithm of the NTRU

cryptosystem, using the public-key polynomial as a key, and using the blind-value polynomial to randomize the verification-value polynomial, to generate an encryption verification-value polynomial as the first cipher text," although Hoffstein et al. do suggest the usage of polynomials and hashing in a public/private key encryption scheme and NTRU, as recited below;

- "the encryption unit generates the encryption information that includes the encryption verification-value polynomial as the first cipher text and the second cipher text," although Hoffstein et al. do suggest the usage of polynomials and hashing in a public/private key encryption scheme and NTRU, as recited below;
- "the different computation algorithm is a symmetric key encryption algorithm," although Hoffstein et al. do suggest the usage of polynomials and hashing in a public/private key encryption scheme and NTRU, as recited below;
- "the second encryption subunit performs the symmetric key encryption algorithm on the seed value using the verification value as a key, to generate the second cipher text," although Hoffstein et al. do suggest the usage of polynomials and hashing in a public/private key encryption scheme and NTRU, as recited below;
- "the different computation algorithm is bitwise exclusive-or," although Hoffstein et al. do suggest the usage of polynomials and hashing in a public/private key encryption scheme and NTRU, as recited below;

- "the second encryption subunit performs the bitwise exclusive-or on the verification value and the seed value, to generate the second cipher text," although Hoffstein et al. do suggest the usage of polynomials and hashing in a public/private key encryption scheme and NTRU, as recited below;
- "the different computation algorithm is addition," although Hoffstein et al. do suggest the usage of polynomials and hashing in a public/private key encryption scheme and NTRU, as recited below;
- "the second encryption subunit performs the addition on the verification value and the seed value, to generate the second cipher text," although Hoffstein et al. do suggest the usage of polynomials and hashing in a public/private key encryption scheme and NTRU, as recited below;
- "the different computation algorithm is multiplication," although Hoffstein et al. do suggest the usage of polynomials and hashing in a public/private key encryption scheme and NTRU, as recited below;
- "the second encryption subunit performs the multiplication on the verification value and the seed value, to generate the second cipher text," although Hoffstein et al. do suggest the usage of polynomials and hashing in a public/private key encryption scheme and NTRU, as recited below;

however, Hoffstein et al. do disclose,

- "She uses this randomly chosen polynomial Θ, Dan's public key h, and her plaintext message m to create the encoded message e using the formula…" [page 16-17];

- "The public key information can be published; that is, made available to any member of the public or to any desired group…" [page 22 lines 12-23];
- "The block 220 represents the routine that can be used by the message sender to encode the plaintext message using the public key of the intended message recipient" [page 22 lines 24-27 & page 23 lines 1-4];
- "a seed-value generating unit operable to generate a seed value," and, "a shared-key generating unit operable to generate a blind value and a shared key, from the seed value" [pages 13-15];
- "1.2 Key Creation. To create an NTRU key…1.3 Encoding…Dan randomly chooses…The polynomial f must satisfy the additional requirement… Dan next computes the quantities… Dan's public key is the list of polynomials… Dan's private key is the single polynomial f…" [page 31];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "the shared-key generating unit performs a one-way function on the seed value, to generate a functional value, and generates a verification value, the blind value, and the shared key, from the functional value" and "the encryption unit includes: a public-key obtaining subunit operable to obtain a public key" and "a first encryption subunit operable to perform a public-key encryption algorithm on the verification value, using the public key and the blind value, to generate a first cipher text" and "a second encryption subunit operable to perform, on the seed value, a computation algorithm different from the public-key encryption algorithm, to generate a second cipher text" and "the encryption unit generates the encryption information that includes the first cipher text and the second cipher text" and "the public-key encryption

algorithm conforms to an NTRU cryptosystem" and "the public-key obtaining subunit obtains a public-key polynomial generated according to a key-generation algorithm of the NTRU cryptosystem, as the public key" and "the first encryption subunit generates a verification-value polynomial from the verification value, generates a blind-value polynomial from the blind value, and encrypts the verification-value polynomial according to an encryption algorithm of the NTRU cryptosystem, using the public-key polynomial as a key, and using the blind-value polynomial to randomize the verification-value polynomial, to generate an encryption verification-value polynomial as the first cipher text" and "the encryption unit generates the encryption information that includes the encryption verification-value polynomial as the first cipher text and the second cipher text" and "the different computation algorithm is a symmetric key encryption algorithm" and "the second encryption subunit performs the symmetric key encryption algorithm on the seed value using the verification value as a key, to generate the second cipher text" and "the different computation algorithm is bitwise exclusive-or" and "the second encryption subunit performs the bitwise exclusive-or on the verification value and the seed value, to generate the second cipher text" and "the different computation algorithm is addition" and "the second encryption subunit performs the addition on the verification value and the seed value, to generate the second cipher text" and "the different computation algorithm is multiplication" and "the second encryption subunit performs the multiplication on the verification value and the seed value, to generate the second cipher text," in the invention as disclosed by Gennaro-066 for the purposes of the encryption/decryption of data according to a NTRU cryptosystem using public keys.

Claims 16-19:

Gennaro-066 disclose a shared-key generation apparatus that notifies a destination apparatus about a shared key in secrecy, as in Claim 3 above, but do not disclose,

- "the seed-value generating unit generates a random number, as the seed value," although Hoffstein et al. do suggest the usage of polynomials and hashing in a public/private key encryption scheme and NTRU, as recited below;
- "the shared-key generating unit performs a one-way function on the seed value, to generate a functional value, and generates the blind value and the shared key from the functional value," although Hoffstein et al. do suggest the usage of polynomials and hashing in a public/private key encryption scheme and NTRU, as recited below;
- "the one-way function is a hash function," although Hoffstein et al. do suggest the usage of polynomials and hashing in a public/private key encryption scheme and NTRU, as recited below;
- "the shared-key generating unit performs the hash function on the seed value," although Hoffstein et al. do suggest the usage of polynomials and hashing in a public/private key encryption scheme and NTRU, as recited below;
- "the shared-key generating unit generates the blind value by setting a part of the functional value as the blind value, and generates the shared key by setting another part of the functional value as the shared key," although Hoffstein et al. do suggest the usage of polynomials and hashing in a public/private key encryption scheme and NTRU, as recited below;

however, Hoffstein et al. do disclose,

- "She uses this randomly chosen polynomial Θ, Dan's public key h, and her plaintext message m to create the encoded message e using the formula…" [page 16-17];
- "a seed-value generating unit operable to generate a seed value," and, "a shared-key generating unit operable to generate a blind value and a shared key, from the seed value" [pages 13-15];
- "1.2 Key Creation. To create an NTRU key…1.3 Encoding…Dan randomly chooses…The polynomial f must satisfy the additional requirement… Dan next computes the quantities… Dan's public key is the list of polynomials… Dan's private key is the single polynomial f…" [page 31];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "the seed-value generating unit generates a random number, as the seed value" and "the shared-key generating unit performs a one-way function on the seed value, to generate a functional value, and generates the blind value and the shared key from the functional value" and "the one-way function is a hash function" and "the shared-key generating unit performs the hash function on the seed value" and "the shared-key generating unit generates the blind value by setting a part of the functional value as the blind value, and generates the shared key by setting another part of the functional value as the shared key," in the invention as disclosed by Gennaro-066 for the purposes of the encryption/decryption of data according to a NTRU cryptosystem using public keys.

Claim 20:

Gennaro-066 disclose a shared-key generation apparatus that notifies a destination apparatus about a shared key in secrecy, as in Claim 3 above, but do not disclose,

- "an obtaining unit operable to obtain a content," although Hoffstein et al. do suggest the usage of polynomials and hashing in a public/private key encryption scheme and NTRU, as recited below;
- "an encryption unit operable to encrypt the obtained content using the shared key, to generate an encrypted content," although Hoffstein et al. do suggest the usage of polynomials and hashing in a public/private key encryption scheme and NTRU, as recited below;
- "wherein the transmitting unit further transmits the encrypted content," although Hoffstein et al. do suggest the usage of polynomials and hashing in a public/private key encryption scheme and NTRU, as recited below;

however, Hoffstein et al. do disclose,

- [Fig 4 Box# 420 illustrates obtaining data/information];
- "The encoding technique of an embodiment of the public key cryptosystem hereof uses a mixing system based on polynomial algebra and reduction modulo two numbers, p and q, while the decoding technique uses an unmixing system whose validity depends on the elementary probability theory" [page 9];
- "Communication is via transceiver…" [page 8 lines 22-24];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "an obtaining unit operable to obtain a content" and "an encryption unit operable to encrypt the obtained content using the shared key, to generate an encrypted content" and "wherein the transmitting unit further transmits the encrypted content," in the invention as disclosed by Gennaro-066 for the purposes of the encryption/decryption of data according to a NTRU cryptosystem using public keys.

Response to Arguments

8. Applicant's arguments, see pages 26-30, filed 04/19/2007, with respect to the rejection(s) of claim(s) 1-39, 41, & 42 under 35 U.S.C. 103(a) have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of Gennaro et al. (US-5937066-A), Gennaro et al. (US-5907618-A), and Hoffstein et al. (WO-9808323-A1), where the inclusion of the two pieces of prior art from Gennaro et al. are intended to provide further details that may be unclear/missing from Hoffstein et al.

Conclusion

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Examiner Oscar Louie whose telephone number is 571-270-1684. The examiner can normally be reached Monday through Thursday from 7:30 AM to 4:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami, can be reached at 571-272-4195. The fax phone number for Formal or Official faxes to Technology Center 2100 is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

OAL
04/09/2008

/Nasser G Moazzami/
Supervisory Patent Examiner, Art Unit 2136